UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/737,306 | 12/15/2000 | Kevin Kwong-Tai Chung | AI-TECH-30 | 1695 |

110 7590 07/13/2004

DANN, DORFMAN, HERRELL & SKILLMAN
1601 MARKET STREET
SUITE 2400
PHILADELPHIA, PA 19103-2307

| EXAMINER | |
|---|---|
| TREMBLAY, MARK STEPHEN | |
| ART UNIT | PAPER NUMBER |
| 2876 | |

DATE MAILED: 07/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/737,306 | CHUNG, KEVIN KWONG-TAI5 | |
| | Examiner | Art Unit | |
| | Mark Tremblay | 2876 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-81 and 83-117* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-81 and 83-117* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/11/04*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *4/30/04* .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Applicant: Chung

Filing date: 12/15/2000

***Response to Amendment***

Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn. Claims 103 - 117, filed 11/17/03, were not treated at the time of the previous office action.

***Claim Rejections - 35 U.S.C. §103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-32, 34, 37-60, 65-68, 71-72, 74-81, and 93-117 are rejected under 35 U.S.C. § 103 as being unpatentable over EP 0419335 to Feterman et al. ("Feterman" hereinafter) in view of well known smart card security techniques. According to the translation by Scientific Translation Services, Feterman discloses a voting system comprising:

a processor (page 5, first paragraph) for processing voting information and providing a unique voting storage zone for each of a plurality of voting sessions;

a display (page 6 paragraph 4) coupled for receiving voting information from said processor;

a voter interface (page 5, second paragraph) for receiving voting selections made by a voter and coupling same to said processor, said processor providing a voting record including the voting selections for each voting session;

a memory (page 5, second through fourth paragraphs) coupled to said processor for storing the voting record for each voting session; and

means (smart cards) coupled to said processor for storing the voting record in the unique voting storage area for each voting session in a tangible medium separate from said memory,

wherein the tangible medium for each voting session is issued (returned to the voter) by said means for storing after the voting record for the voting session is stored in the unique storage area and before a next voting session.

Feterman discloses different options or examples, 2-4 (page 8), usable together, in which the voting booth and ballot box are combined, cards are not used by multiple voters, and the activation of the storage zones takes place when the voter confirms his vote. Such a construction of the reference leads to the concept of a stand alone voting machine.

Feterman discloses a randomly chosen storage area to prevent the matching of a voter with a particular vote cast, while still providing for recounts and ballot integrity. Clearly, this is not as important in a system where cards are not reused, as there would be a one to one correspondance between voters and a single card.

Feterman chooses a smart card system, which is notoriously well known for providing security and, if desired, anonymous transactions. However, Feterman does not even mention security protocols commonly used in smart card systems, much less describe them. This is presumably because the security protocols used with smart cards were well known at the time the invention was made. For example, in the one case where Feterman allows one card to carry 48 votes, how does Feterman prevent a person knowledgable about smart cards from switching the smart card they are given,

which has votes recorded from up to 48 previous voters, with a card that has 48 votes chosen for one candidate? How does Feterman prevent person from introducing a smart card which is programmed to change votes, to selectively not record votes, or perform some other mischief, sabotage, or corruption? Or, how does Feterman prevent a person from reading the votes on the card when they go in the voting booth, if they are carrying a portable smart card reader which can be purchased on the open market? 48 votes might be coerced if the coercer verifies with a portable smart card reader that all preceding 48 votes are cast for the coercer's choice. What about the introduction of viruses and worms into the system, using a rogue smart card?

Feterman doesn't need to cover these things because they were known in the art from at least the early eighties. Security on a smart card is standard, rather than an option. If security were not required, a smart card would not typically be required; a simple memory card, magnetic stripe card, or bar code would suffice. Since smart cards were invented in France in the 1970s, and security was a raison d'etre for smart cards, it follows that security was well established by the year 2000. Examiner has cited chapters from four text books (three titled "Smart Cards" and a fourth titled "Smart Card Handbook") dealing with smart card security, as a way of establishing security techniques known to one of ordinary skill in the art. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to use known security techniques to protect the smart cards in Feterman from unauthorized uses and substitutions.

There are numerous ways in which the application of security techniques known in the art lead to the storage of a number which would be identified as, be used as, and/or be equivalent to a unique voting session identifier.

Zoreda teaches that a number of security techniques are in use in smart cards. At page 43, for example, Zoreda teaches, "Smart cards use encryption process to carry out several tasks. Many card modules include DES as a built-in feature." In other words, DES encryption is so common in smart cards, DES routines often hard-wired right into the card, rather than programmed in by the user. Zoreda also teaches of a process for verifying the card and external system are authorized to work together,

called a challenge. This involves the use of a random number. Storing this number for the purpose of later proving that the card had been properly authenticated to the reader would provide the equivalent of a unique voting session identifier. Zoreda also teaches the use of digital signatures, which are unique numbers appended to a message (in this case, a voters choices) that cannot be forged and provides a means for non-repudiation of the message.

The Smart Card Handbook by Rankl and Effing ("Rankl" hereinafter) provides a somewhat more comprehensive treatment of smart card security. Rankl teaches both challenge/response and digital signatures mentioned above. Rankl has a long session on Random numbers that contains the statement at page 84 "Typical applications in the field of Smart Cards are ensuring the uniqueness of a session during authentication..." Thus, Rankl clearly and plainly states that random numbers are typically used as unique session identifiers in smart cards during authentication. Rankl also teaches other security methods that are relevant, such as "dynamic keys" (also called session keys) at page 258.

"Smart Cards Seizing Strategic Business Opportunities" edited by Allen et al. ("Allen" hereinafter) provides a useful chapter on smart card security. A table at page 260 lists common attacks and counter-attacks. Among attacks is "copied identity" which may be countered by "check physical transaction location". This appears to be similar to a solution suggested by Feterman. But there are numerous other types of attacks listed. Counter attacks include "random numbers", "transaction counters", "non-repudiation signatures" and "cryptographic signatures", all of which can be construed as the same as, equivalent to, or useful as a unique session identifier.

"Smart Cards A Guide to Building and Managing Smart Card Applications" By Dreifus and Monk ("Dreifus" hereinafter") also has a useful chapter on System and Data Integrity. This is clearly important in any electronic voting system, and clearly important in the field of smart cards. Dreifus teaches that the storage of data in several locations is critcal to data integrity. One element is transaction logs. Dreifus teaches that a log of a transaction may be stored on a terminal, a host system, in the smart card, and on a paper log. Dreifus teaches that unique batch sequence numbers, "unique identification

numbers for each transaction" prevents attempts to defraud the system by double posting (the same as double voting, a clear no-no). Dreifus teaches that all of these techniques should be used together because the card can fail, the host can fail, the central system can fail, and all are suseptible to attempts to defraud them.

Re claim 10, the "ballot box" suggests a container for the smart cards.

Re claims 111-112, this is commonly known in the art of providing a paper log, and would be understood from the Dreifus teaching.

Claims 33, 35, 36, 69-70, 73 are rejected under 35 U.S.C. § 103 as being unpatentable over Feterman in view of well known smart card security techniques, further in view of U.S. Patent #6,081,793 to Challener et al. ("Challener" hereinafter). Feterman teaches a voting apparatus as described above, but does not teach the use of a voting system on the Internet. The cited teachings on smart card security clearly teach that attempts to defraud a smart card system such as Feterman can be defeated. Feterman does not teach a voting system used on the Internet. Challener teaches that the "rising importance of the Interenet and other forms of electronic communication in the United States of America and abroad presents a unique opportunity to reduce the inconvenience and expense associated with tratidional voting systems. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to use a secured system such as Feterman to provide Internet voting, because the Interenet reduces the inconvenience and expense associated with traditional voting systems, as taught by Challener.

Claims 61-64 are rejected under 35 U.S.C. 103 as being unpatentable over Feterman in view of well known smart card security techniques, and further in view of 1998 Advanced Card Technology Sourcebook ("Sourcebook" hereinafter). Feterman as modified teaches the features of the invention, but do not teach the larger sizes of the storage on smart cards. Sourcebook teaches that 32K cards were feasible in 1997, and

predicted to increase to 64K by 1999. Sourcebook also teaches that large EEPROMs are desirable, since applications can be loaded and deleted in a secure fashion onto them. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to provide a smart card having at least 32K, at least because such a smart card is more versatile and adaptable to multiple applications, as understood in the art, making the voter card more versatile, and useful for other applications. There are as many reasons to want larger storage size on a smart card, as there is for wanting more storage on a PC.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

***Voice***

Inquiries for the Examiner should be directed to Mark Tremblay at (571) 272-2408. The Examiner's regular office hours are 10:30 am to 7:00 pm EST Monday to Friday. Voice mail is available. Technical questions and comments concerning PTO procedures may be directed to the Patent Assistance Center hotline at 1-800-786-9199 or (703) 308-4357.

MARK TREMBLAY
PRIMARY EXAMINER

June 24, 2004